REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Change of Address

Applicant advises that correspondence continues to be sent to the previous address on record (at McCarthy Tetrault) rather than to the address specified for customer number 27871. A Change of Correspondence Address form was filed on April 4, 2005. Applicant requests that the Office kindly update its records to reflect same so that future correspondence will be sent to Blake, Cassels & Graydon (i.e. customer 27871).

Commentary re Final Rejection

Firstly, Applicant respectfully requests clarification regarding the alleged "new" grounds for rejecting the claims. Applicant believes that the rejections under 35 U.S.C. 102(e) in view of Boden are substantially the same as those outlined in the Office Actions dated June 22, 2005 and January 13, 2006. As such, it is unclear what new grounds of rejection have been formulated.

Applicant notes that the previous amendments were made to clarify the distinctions over Boden that were previously argued. In particular, the claims now emphasize that the software module intercepts and operates on packets transparent to the public host. This was clearly outlined in Applicant's previous response, however, the Examiner does not seem to address this new language in the Office Action presently addressed, let alone point to passages in Boden that teach such limitations.

Applicant believes that the Examiner has overlooked the new language in the claims and thus has not fully considered Applicant's previous arguments. As such, it is believed that the finality of the present office action should be withdrawn so that the Examiner can fully consider the amendments filed on June 28, 2006 and how these amendments distinguish over Boden.

Claim Rejections

Claims 1-4 and 12-19 have again been rejected under 35 U.S.C. 102(e) as being anticipated by Boden. Applicant again traverses the rejections, and for the Examiner's convenience, has reiterated the previous arguments below.

The present application relates to a system and method for transparently resolving a web site address for a public host when the public host is connected to a virtual private network. The public host includes a software module that monitors, intercepts and routes domain name requests and subsequent responses without the public host knowing that such an operation is occurring, i.e. transparent thereto.

This "interception" is performed at the host, i.e., communication packets outbound from the host toward the gateway are intercepted, operated on and then routed without the public host knowing. Claim 1 has been amended to clarify the transparency of the software module to the public host. Such transparency is particularly useful where the system parameters of the public host are not alterable, e.g., where the public host will only receive address locations from the ISP DNS (e.g. see page 4, lines 14-23). In the present application, when the public host is connected to a VPN, it is also able to receive address locations from the VPN DNS while thinking that it is receiving address locations from the DNS of the ISP.

Claim 1, as amended, specifies that the modification of the requests outbound of the public host occurs by the software module replacing an address of the ISP DNS with the address of the DNS of the VPN. The DNS of the VPN may then resolve the request and return a domain name response. In order to fool the public host into thinking that it is receiving an address location from the DNS of the ISP, the software module also modifies inbound responses to counter-act the address modification. The software module operates to transparently route domain name requests in a host-to-gateway connection.

Boden teaches a system for integrating network address translation (NAT) with internet protocol (IP) security. Security is provided in a VPN by performing one or a combination of four types of VPN NAT. This procedure involves dynamically generating NAT rules and associating them with the manual or dynamically generated security associations before beginning IP security that uses the security associations. As IP Sec is performed on outbound and inbound datagrams, the NAT function is also performed on a gateway-to-gateway connection. Boden is concerned with avoiding duplication of the DNS entries on DNS servers and to avoid possible conflicts with IP addresses (overlapping address domains).

Boden does not teach transparent routing on a host-to-gateway connection but rather operates purely at a gateway-to-gateway connection. The user (host) is at all time aware (and in fact participates in configuring) NAT occurs.

Applicant refers to column 5, lines 64-67, which clearly shows that in Boden, the NAT operations are not transparent to the host (user) but in fact are configured by the users themselves: "In step 20, the user decides on and configures the connections that will require NAT. This is logically equivalent to writing NAT rules. The four cases to be considered in doing so are depicted in Table 1." As noted above, claim 1 has been amended to more clearly express that the software module is included in (i.e. at host) and operates transparent to the public host, which is believed to further clarify this distinction over Boden.

Therefore, Boden does not teach a software module at the public host transparently intercepting and modifying domain name requests but rather teaches NAT in a gateway-to-gateway connection and the user actually actively participates in configuring the NAT rules. For at least this reason, Boden does not teach every element of claim 1 and, as such clearly cannot anticipate.

As noted above, claim 1 is also amended to specify how the software module modifies the request, namely by replacing an ISP DNS address with a VPN DNS address, previously part of claim 12. Applicant respectfully submits that Boden does not teach such a step and thus cannot anticipate.

The Examiner relies on column 6, line 60 to column 7, line 36 in support of teaching the subject matter of previous claim 12. However, upon a careful review of this passage, Applicant cannot determine where in Boden the Examiner has located such a step. If anything, Boden teaches a gateway replacing an address, i.e., during NAT.

Applicant respectfully submits that Boden does not teach a software module at the public host modifying a domain name request as claimed. Therefore, for at least this reason, Applicant believes that Boden cannot anticipate amended claim 1.

As shown above, Applicant believes that the amendments made to claim 1 serve to clarify the distinctions over Boden. In particular, where claim 1 is concerned with transparently routing domain name requests in a host-to-gateway connection, Boden in fact has the host participate in configuring NAT rules. Further, where claim 1 includes a step of the software module at the public host modifying an address in the request, Boden is entirely silent in that regard and at most teaches a visible address modification at the gateway. Therefore, Applicant believes that amended claim 1 clearly distinguishes over Boden and that the rejections under 35 U.S.C. 102(e) are improper.

Applicant requests early reconsideration and allowance of the present application. Applicant invites the Examiner to contact the undersigned should they wish to discuss any of the above issues in light of the finality of the rejections.

Respectfully submitted,

Brett J. Slaney
Agent for Applicant
Registration No. 58,772

Date: November 7, 2006

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.2518
BS/